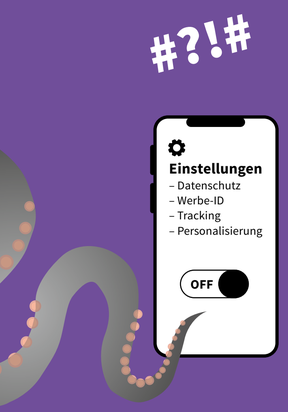
Tipps für deinen Schutz – Datenschutzfreundliche Einstellungen für Smartphones, Tablets und Notebooks



Tipps zum Schutz

1. Pass auf deinen Geräten die Einstellungen zum Datenschutz an und schalte sie ein. Die Einstellungen zum Tracking und zur Personalisierung, sowie die Werbe-ID solltest du abschalten!
2. Verwende komplexe Passwörter: mindestens acht Zeichen aus Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen!
3. Installiere regelmäßig Updates und sorge für einen Virenschutz! Sichere deine Daten regelmäßig durch ein Backup!
4. Richte die Verschlüsselung deiner Geräte und der externen Speichermedien (z. B. SD-Karte, USB-Stick etc.) ein.
5. Überprüfe die Zugriffsberechtigungen deiner Apps (z. B. Übermittlung der Standortdaten deaktivieren)!
6. Wähle geschützte Kommunikationswege. Achte beim Browser auf eine „https“-Adresse und bei deinem Messenger auf eine Ende-zu-Ende Verschlüsselung!
7. Aktiviere die Bildschirmsperre bei deinem Laptop! Richte eine PIN bei deinem Smartphone und deinem Tablet ein!
8. Sichere deine Daten regelmäßig durch ein Backup!
9. Sei vorsichtig beim Öffnen von E-Mail-Anhängen und Links! Schau dir genau an, worauf du klickst und was du herunterlädst. Es kann sich um Schadsoftware handeln!
10. Schütze deine SIM-Karte mit einer PIN!

#verschlüsselung
Richte die Verschlüsselung deiner Geräte und der Speichermedien (z.B. SD-Karte, USB-Sticks etc.) ein. Du kannst einstellen, dass die Geräte und auch die Festplatten verschlüsselt werden!

Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Impressum
Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland

Lange Laube 20
30159 Hannover

Telefon: +49 (0) 511 768128-0
Telefax: +49 (0) 511 768128-20
E-Mail: info@datenschutz.ekd.de
Internet: datenschutz.ekd.de

Gestaltung: adconcept werbeagentur gmbh und Bureau Sebastian Moock
Druck: QUBUS media GmbH
Stand: Dezember 2022

④ Betroffenenrechte

Wenn personenbezogene Daten einer Person verarbeitet werden, hat diese betroffene Person bestimmte Rechte (Betroffenenrechte). Die Betroffenenrechte sind im *EKD-Datenschutzgesetz* geregelt. Dabei macht es keinen Unterschied, ob die personenbezogenen Daten digital (z. B. in Social Media) oder analog verarbeitet werden. Die Pflichten im Umgang mit personenbezogenen Daten ergeben sich für Privatpersonen nicht direkt aus dem *EKD-Datenschutzgesetz,* sondern aus zivilrechtlichen oder strafrechtlichen Vorschriften oder dem Urheberrecht.

Recht auf Privatsphäre
Das *Recht auf Privatsphäre* muss von anderen Personen geachtet werden. Geschützt wird die *Privatsphäre* durch das *allgemeine Persönlichkeitsrecht* aus Art. 2 Absatz 1 des *Grundgesetzes.* Dort heißt es: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“ Dieser Artikel ist in Verbindung mit Art. 1 Absatz 1 Grundgesetz zu sehen: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“ Es ist also im *Grundgesetz* geregelt, dass sich jeder Mensch in einem persönlichen Bereich frei und ungezwungen verhalten kann, ohne Angst haben zu müssen, durch Dritte beobachtet und abgehört zu werden. Zum geschützten Bereich gehört auch die *Intimsphäre* eines jeden Menschen. Der Staat kann daher z. B. nicht einfach auf Tagebuchaufzeichnungen zugreifen. Das wäre nur unter ganz bestimmten Bedingungen als Ausnahme möglich, zum Beispiel, wenn es zur Aufklärung einer Straftat notwendig ist. Auch die *Geheimsphäre* eines jeden Menschen ist geschützt. Es dürfen keine Äußerungen eines Menschen veröffentlicht werden, wenn dem nicht ausdrücklich zugestimmt wurde. Das betrifft auch Telefongespräche (Fernmeldegeheimnis) oder persönliche Briefe (Briefgeheimnis). Auch hier gibt es nur wenige Ausnahmen, die den Staat berechtigen, von diesen Grundsätzen abzuweichen.

Recht am eigenen Bild
Das *Recht am eigenen Bild* bedeutet, dass jede Person zu jeder Zeit selbst darüber entscheiden darf, ob und wann Aufnahmen von ihr veröffentlicht werden. Das ist Inhalt des *Kunsturhebergesetzes.* Man braucht daher in der Regel eine Zustimmung der Person, deren Foto oder Video veröffentlicht oder im Internet gepostet werden soll. Von diesem Grundsatz gibt es einige wenige Ausnahmen. Eine Ausnahme gilt z. B. für die Veröffentlichung von Fotos von Personen des öffentlichen Lebens wie Politikerinnen oder Schauspieler. Auch Bilder von Versammlungen, Aufzügen und ähnlichen Veranstaltungen dürfen unter Umständen ohne eine Einwilligung der abgelichteten Personen verbreitet werden. Wer das *Recht am eigenen Bild* missachtet, begeht eine Straftat und kann eine Geld- oder Freiheitsstrafe riskieren. Daher ist Achtsamkeit beim Teilen von Fotos und Videos und die Nutzung datenschutzkonformer Kommunikationswege ganz entscheidend.

Auskunftsrecht
Das *EKD-Datenschutzgesetz* regelt, dass Personen, deren Daten von evangelischen Einrichtungen (Schulen, Kindergärten, Krankenhäuser oder Kirchengemeinden etc.) verarbeitet werden, ein *Recht auf Auskunft* darüber haben, welche Daten genau von ihnen gespeichert werden. Die betroffene Person kann also bei der verarbeitenden Stelle anfragen, welche personenbezogenen Daten über sie gespeichert sind. Die jeweilige Einrichtung muss dann mitteilen, welche Daten sie gespeichert hat und zu welchem Zweck diese Daten benötigt werden. Außerdem muss sie die gesetzliche Grundlage nennen, welche sie zur Verarbeitung der Daten berechtigt.

Recht auf Löschung
Betroffene Personen haben nach dem *EKD-Datenschutzgesetz* außerdem das Recht, dass von der verarbeitenden Stelle alle Daten zur eigenen Person gelöscht werden, wenn diese falsch sind oder es keinen Grund mehr gibt, diese Daten (weiter) aufzubewahren. Daher heißt dieses Recht auch das *Recht auf Vergessenwerden.*

Recht auf Beschwerde
Für den Fall, dass gegen das *EKD-Datenschutzgesetz* verstoßen wird, kann jede betroffene Person eine Beschwerde bei der zuständigen Datenschutzaufsichtsbehörde einlegen. Dies ist im Bereich der evangelischen Kirche in vielen Fällen der Beauftragte für den Datenschutz der EKD (BfD EKD). Weitere Informationen können der Homepage des BfD EKD unter https://datenschutz.ekd.de/ entnommen werden.

③ Datenschutzeinstellungen

Smartphones, Tablets, Notebooks etc. entsprechen in der Regel im Auslieferungszustand nicht den Anforderungen des Datenschutzes. Zum Schutz müssen daher die Einstellungen der technischen Geräte in der Regel angepasst werden. Nur so wird ein Mindestmaß an Datenschutz und IT-Sicherheit erreicht. Die notwendigen Anpassungen können in den entsprechenden Systemeinstellungen zur Sicherheit und zum Datenschutz vorgenommen werden. Je strenger diese Einstellungen gewählt werden, desto besser sind die eigenen personenbezogenen Daten geschützt.

Programme und Apps
Programme und Apps sollten so eingestellt werden, dass sie möglichst wenige Daten sammeln. Das gilt ganz besonders für den täglich genutzten Browser. Datenschutzfreundliche Browser unterstützen auch das automatische Löschen von Cookies. Das ist zum Beispiel mit Firefox oder Brave gut umsetzbar. Bei den Apps auf dem Smartphone müssen die Zugriffsberechtigungen genau überprüft und eingeschränkt werden (z. B. Standortdatenübermittlung deaktivieren). So erhalten Fremde keine weitergehenden Informationen. Apps sollten außerdem nur aus vertrauenswürdigen Quellen installiert werden (Playstore/App-Store). Bei Kindern ist es zusätzlich wichtig, besondere Schutzvorkehrungen zu treffen. Dazu gehören Programme, die Jugendschutzeinstellungen vornehmen und die Nutzungszeit beschränken.

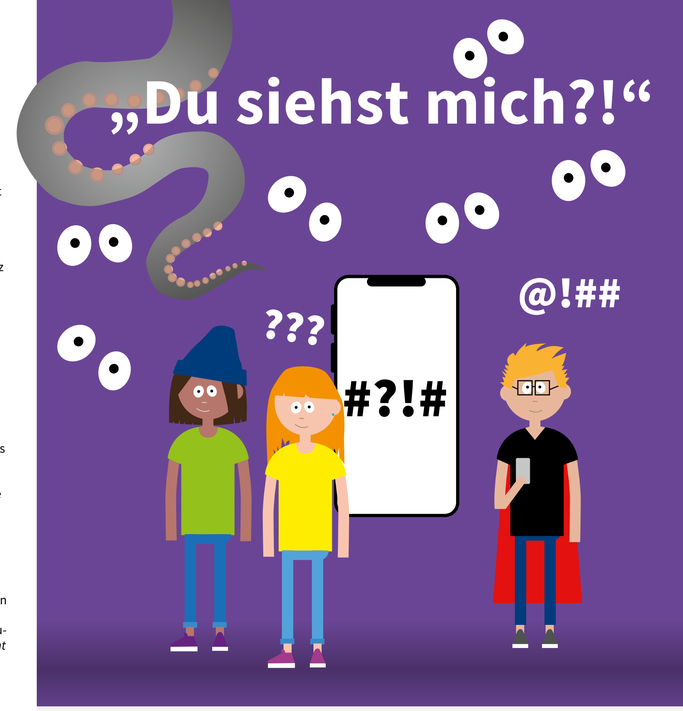
Passwörter
Komplexe Passwörter zu wählen, ist sehr wichtig – und jeder Account sollte tatsächlich ein eigenes Passwort haben! Mindestens acht Zeichen aus vier verschiedenen Zeichenarten sind hier empfehlenswert: kleine und große Buchstaben sowie Zahlen und Sonderzeichen. Da sich die meisten Menschen ihre unterschiedlichen Passwörter nicht merken können, ist die Benutzung eines Passwortmanagers zu empfehlen.

Backups zur Datensicherung
Durch die regelmäßige Durchführung von Datensicherungen (Backups) werden alle Daten gesichert und vor einem Datenverlust geschützt. Diese Backups sollten an einem sicheren Ort gelagert werden. Speicherorte im Internet (Cloudspeicher) ohne Verschlüsselung und ohne ausreichenden Zugriffsschutz (Benutzer-Authentifizierung) sind kritisch zu beurteilen und sollten auf gar keinen Fall für sensible Informationen genutzt werden. Auch Cloudspeicher sollten daher durch Passwörter gesichert werden.

Sichere Kommunikation und Verbindung
Damit die Kommunikation vor Zugriffen von Fremden geschützt wird, sollten nur verschlüsselte und bekannte WLAN-Verbindungen genutzt werden. Da WLAN und auch Bluetooth unbeabsichtigt Informationen preisgeben können, sollten diese Verbindungen außerdem nur bei Bedarf angeschaltet werden. Ein VPN-Tunnel hilft, den eigenen Datenverkehr vor dem Ausspähen durch Fremde zu sichern. Der Internet-Browser sollte immer über verschlüsselte Verbindungen kommunizieren. Diese können an dem Schloss-Symbol in der Browser-Zeile erkannt werden. Sichere Verbindungen beginnen immer mit „https“. Achtung: Die Kommunikation per E-Mail erfolgt meistens nur transportverschlüsselt und ermöglicht somit den E-Mail-Providern das Lesen und Auswerten der übermittelten Daten einschließlich der Anhänge. Dies kann nur verhindert werden, wenn die Inhalte und Anhänge Ende-zu-Ende verschlüsselt werden. Welches Verfahren dazu genutzt wird, müssen Sender und Empfänger vorher vereinbaren. Als Alternative haben sich Messenger mit einer bereits vorhandenen Ende-zu-Ende-Verschlüsselung etabliert. Allerdings sind nur Messenger zu empfehlen, die den Datenschutz ausreichend beachten. Einen Schutz vor Angriffen aus dem Internet bieten Firewalls. Es gilt daher darauf zu achten, dass diese Firewalls auch eingeschaltet sind. Gute Firewalls bieten sogar Einstellungsmöglichkeiten zum Jugendschutz.

Schadsoftware
Häufig werden unbeabsichtigt Schadprogramme installiert. Besondere Vorsicht ist daher beim Empfang von Nachrichten mit Anhängen geboten (Stichwort „Phishing“). Viele verschiedene Anhänge können Schadsoftware enthalten und sollten daher auf keinen Fall ohne Prüfung geöffnet werden. Schadcode verbirgt sich oft auch in Dokumenten mit Makros. Deshalb sollten Makros aus fremden Dokumenten nicht ausgeführt werden. Auch in der Nachricht selbst können Links verschickt werden, die dann zu Servern mit Schadcode führen. Die angezeigten Links können ganz einfach gefälscht sein. Auch übermäßig lange Links verschleiern den Weg zum eigentlichen Absender. Nur ein Blick in die Verknüpfung zeigt den tatsächlichen Weg zum Server. Deshalb: Vorsicht beim Öffnen von Anhängen und Links!

Eine Übersicht der Tipps zu datenschutzfreundlichen Einstellungen für Smartphones, Tablets und Notebooks befindet sich auf dem umseitigen Poster.



#datenschutz

Gesehen zu werden, ist oft etwas Gutes! Aber manches möchten wir nicht preisgeben! Das kann ganz besonders für Daten und Informationen über uns selbst gelten. Da möchten wir gern selbst bestimmen, wer was über uns weiß. Der Schutz meiner Daten betrifft also mich selbst!

Hier findest du einen Einstieg in das Thema und Tipps zum Datenschutz und zur Datensicherheit.

Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

① Einführung in den Datenschutz

Der Datenschutz dient in erster Linie dem Schutz von Menschen und ihrer persönlichen Daten. Die rechtliche Grundlage des Datenschutzes ist das sogenannte *Recht auf informationelle Selbstbestimmung*, welches aus dem *allgemeinen Persönlichkeitsrecht* im Grundgesetz abgeleitet wird. Daher werden juristische Personen – also etwa Unternehmen oder Vereine – durch den Datenschutz nicht geschützt. Der Schutz bezieht sich immer auf personenbezogene Daten. Das sind alle Daten, die einem einzelnen Menschen zugeordnet werden können – also etwa unser Name oder unser Geburtsdatum. Es gibt auch besondere Kategorien personenbezogener Daten. Diese Daten beziehen sich zum Beispiel auf unsere Gesundheit, auf unsere politische Einstellung oder unser Sexualleben. Solche Daten sind besonders schützenswert und die Verwendung unterliegt höheren Anforderungen. Auch Informationen, die Menschen im Rahmen eines vertraulichen Gesprächs preisgeben, zum Beispiel im Rahmen eines Seelsorge- oder Beratungsgesprächs oder bei einer ärztlichen Behandlung, fallen unter den Datenschutz.

Im Bereich der Evangelischen Kirche in Deutschland gibt es ein eigenes Datenschutzgesetz, das Datenschutzgesetz der Evangelischen Kirche in Deutschland, kurz *EKD-Datenschutzgesetz.* Der Hintergrund eines eigenen Kirchengesetzes ist zum einen die historisch gewachsene und im Grundgesetz geschützte Stellung der Kirchen und zum anderen die jahrhundertealte Tradition der Kirchen zur Verschwiegenheit im Rahmen der Seelsorge und der Beichte. Deshalb ist es der evangelischen Kirche möglich, sich ein eigenes Datenschutzgesetz zu geben, wovon sie bereits seit 1978 Gebrauch macht. Die *europäische Datenschutzgrundverordnung (DSGVO)* regelt in Art. 91, dass eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft eigene Regelungen anwenden darf, sofern diese im Einklang mit der DSGVO stehen. Das *EKD-Datenschutzgesetz* gilt für alle evangelischen Einrichtungen in Kirche und Diakonie (z. B. evangelische Schulen, Krankenhäuser, Kindergärten, Kirchengemeinden uvm.). Personenbezogene Daten müssen daher von allen hauptamtlichen, beruflichen und ehrenamtlichen Mitarbeitenden einer kirchlichen oder diakonischen Einrichtung vertraulich behandelt werden, denn für sie gilt das Datengeheimnis.

② Unbewusstes Datensammeln

Mittlerweile ist die Nutzung des Internets aus unserem Alltag nicht mehr wegzudenken. Bei der Arbeit, der Recherche für die Schule oder für die ehrenamtliche Arbeit in Vereinen und im Konfirmandenunterricht werden häufig entweder das Internet oder auch gezielt nützliche Apps herangezogen. Beim Besuch von Internetseiten werden in der Regel automatisch personenbezogene Daten gespeichert. Das können unter anderem die IP-Adresse, genaue Standortdaten, die genutzte Sprache oder auch Daten zum Nutzungsverhalten sein. Diese Daten können eingesetzt werden, um Internetseiten zu optimieren oder um gezielt nutzerbezogene Angebote oder Informationen zu zeigen, z. B. die sogenannte „personalisierte Werbung“. Beim „liken“ von Produkten oder Artikeln auf Plattformen wie Facebook oder Instagram wird dies im Hintergrund registriert und dazu genutzt, Profile der Nutzenden zu erstellen. Weil solche Informationen auch kommerziell genutzt werden, tauchen dann in den Internet-Suchmaschinen passgenau zugeschnittene Werbeangebote auf. Personenbezogene Daten sind also sehr wertvoll und werden bereits als „Währung“ gehandelt. Deshalb werden soziale Netzwerke wie Facebook, TikTok oder Instagram häufig auch als „Datenkraken“ bezeichnet. Sie sammeln heimlich und unbemerkt im Hintergrund umfangreiche Informationen und kennen so die Vorlieben und Hobbies, die Freunde, die politische Einstellung und die religiöse Auffassung der Internetnutzer. Gesetzlich ist aber vorgeschrieben, dass auf die Daten auf Internetseiten und in Apps nur dann zugegriffen werden darf, wenn in die Datenverarbeitung ausdrücklich eingewilligt wurde. Das heißt, die Daten dürfen nur gesammelt werden, wenn ausdrücklich der Sammlung und Nutzung dieser Daten zugestimmt wurde. Davon gibt es nur wenige Ausnahmen. Es ist also wichtig, immer genau zu prüfen, welche Daten jede und jeder Einzelne wo über sich preisgeben möchte. Gerade im Umgang mit Apps ist besondere Vorsicht geboten.

„Du siehst mich?!“

#briefgeheimnis
Briefe und Pakete darf nur der Adressat öffnen. Die Botschaft im Umschlag ist geheim – und dieses Geheimnis darf von anderen nicht verletzt werden. Das Briefgeheimnis ist sogar im Grundgesetz verankert!

#vertrauliche_gespräche
Vertrauliche Gespräche gehören nicht an öffentliche Orte. Schütze dich und andere, indem du rücksichtsvoll handelst! Wer Gespräche mit dem Smartphone aufnimmt, ohne dass die anderen davon wissen, kann sich strafbar machen!

#recht_am_eigenen_bild
Das Recht am eigenen Bild wird aus dem allgemeinen Persönlichkeitsrecht im Grundgesetz abgeleitet. Es besagt, dass jede Person selbst bestimmen darf, ob überhaupt und in welchem Zusammenhang Aufnahmen wie Fotos oder Videos von ihr oder ihm veröffentlicht werden. Poste nicht ungefragt Fotos oder Videos, auf denen andere Personen abgebildet sind!

#social_media
Auch in sozialen Netzwerken gelten Regeln! Das Internet ist kein rechtsfreier Raum. Kommentare und Posts sind schnell über das Netz verschickt. Hate Speech und Cybermobbing sind sogar strafbar. Verhalte dich deshalb auch im Netz fair und achte die Rechte anderer!

#konfirmandenunterricht
„Du bist ein Gott, der mich sieht.“ So steht es in der Bibel in 1. Mose 16, 13. Wahrgenommen zu werden, ist etwas Gutes. Mit allen Informationen von vielen Menschen gesehen zu werden, hingegen nicht unbedingt. Jede und jeder darf über die eigenen Daten selbst verfügen! Achte daher auch die Rechte deiner Mitkonfirmandinnen und Mitkonfirmanden!

#cookies
Cookies sind kleine Dateien, die dauerhaft oder für eine bestimmte Zeit auf deinem Endgerät gespeichert werden. Es gibt technische Cookies, die notwendig sind und das Surfen erleichtern. Es gibt aber auch Werbe- oder Tracking-Cookies, die nicht ohne deine ausdrückliche Zustimmung gesetzt werden dürfen!

#tagebuch
Ein Tagebuch zeichnet Erlebnisse nach. Dort hältst du Erinnerungen fest und fängst Momente ein. Du bildest ab, was passiert ist und erzählst deine Geschichte. Du entscheidest, mit wem du deine Geschichte teilst!

#standortfreigabe
Viele Apps möchten auf deine Standortdaten zugreifen. Überlege dir gut, mit wem du deinen Standort teilen möchtest. In den Einstellungen kannst du die Übermittlung der Standortdaten deaktivieren!

#datenschutz

Gesehen zu werden, ist oft etwas Gutes! Aber manches möchten wir nicht preisgeben! Das kann ganz besonders für Daten und Informationen über uns selbst gelten. Da möchten wir gern selbst bestimmen, wer was über uns weiß. Der Schutz meiner Daten betrifft also mich selbst!

Hier findest du einen Einstieg in das Thema und Tipps zum Datenschutz und zur Datensicherheit.

Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Impressum
Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland

Lange Laube 20
30159 Hannover

Telefon: +49 (0) 511 768128-0
Telefax: +49 (0) 511 768128-20
E-Mail: info@datenschutz.ekd.de
Internet: datenschutz.ekd.de

Gestaltung: adconcept werbeagentur gmbh und Bureau Sebastian Moock
Druck: QUBUS media GmbH
Stand: Dezember 2022